IN THE SPECIFICATION

Please amend paragraph 0002 at page 1 as follows. (The three changes are in the second line and the next to last line of the paragraph below.)

[0002] A computer network typically comprises a plurality of interconnected devices~~,~~. These devices may include any network device, such as a server or end station, that transmits or receives data frames. A common type of computer network is a local area network ("LAN") which typically refers to a privately owned network within a single building or campus. LANs may employ a data communication protocol, such as Ethernet or token ring, that defines the functions performed by the data link and physical layers of a communications architecture in the LAN. In many instances, several LANs are interconnected by point-to-point links, microwave transceivers, satellite hook-ups, etc. to form a wide area network ("WAN")~~,~~ that may span an entire country or continent.

Please amend paragraph 0003 at pages 1-2 as follows. (The one change is in the last line of the paragraph below.)

[0003] One or more intermediate network devices are often used to couple LANs together and allow the corresponding entities to exchange information. For example, a bridge may be used to provide a bridging function between two or more LANs. Alternatively, a switch may be utilized to provide a switching function for transferring information among a plurality of LANs or end stations. In effect, a switch is a bridge among more than two networks or entities. The terms "bridge" and "switch" will be used interchangeably throughout this description. Bridges and switches are typically devices that operate at the Data Link

layer ("layer 2") of the Open Systems Interconnection ("OSI") model. Their operation is defined in the American National Standards Institute ("ANSI") Institute of Electrical and Electronics Engineers ("IEEE") 802.1D standard. A copy of the ANSI/IEEE Standard 802.1D, 1998 Edition, is incorporated by ~~referenced~~ reference herein in its entirety.

Please amend paragraph 0005 at page 2 as follows. (The three changes are in the second, forth, and sixth lines of the paragraph below.)

[0005] Networks may be designed using a plurality of distinct topologies - that is, the entities in the network may be coupled together in many different ways. Referring to Figs. 1 - 3, there ~~is~~ are shown different examples of "ring" topologies. A ring topology is a network configuration formed when "Layer 2" bridges are placed in a circular fashion, with each bridge having two and only two ports belonging to a specific ring. Fig. 1 shows a single ring 150 having bridges 152 connected by paths 154. Each bridge 152 in ring 150 in Fig. 1 has two ports 152a and 152b belonging to the ring. Fig. 2 shows two adjacent rings, 150a and 150b, with a single bridge 156 having two ports 156a, 156b belonging to each ring.

Please amend paragraph 0016 at page 6 as follows. (The changes are in the fifth line of the paragraph below.)

[0016] Other available loop avoidance protocols include that shown and described in now pending NETWORK CONFIGURATION PROTOCOL AND METHOD FOR RAPID TRAFFIC RECOVERY AND LOOP AVOIDANCE IN RING TOPOLOGIES, filed March 4, 2002, serial number 10/090,669, now U.S. Patent No. 6,717,922, issued April 6, 2004,

and now pending SYSTEM AND METHOD FOR PROVIDING NETWORK ROUTE REDUNDANCY ACROSS LAYER 2 DEVICES, filed April 16, 2002, serial number 10/124,449. The entirety of these applications ~~are~~ is hereby incorporated by reference.

Please amend paragraph 0018 at pages 6-7 as follows. (The two changes are in the eleventh and twelfth lines of the paragraph below.)

[0018] To illustrate this problem, referring to Fig. 5, there is shown a network 180 comprising a core or higher priority network such as a provider 170 coupled to a customer or lower priority network 172 with a lower priority through a switch 174. Core network 170 runs a conventional spanning tree protocol to avoid loops and has defined a blocked path 176. This means that either port 178 or port 180 is blocked. Many different causes may result in involuntary loops which may collapse the entire network 180 including: STP corrupted BPDUs, unidirectional optical fibers which result, for example, when paths which typically comprise two optical fibers ~~but one has~~ have one optical fiber shut down, and non-configured protocols in loop topologies. In the example in Fig. 5, someone in customer network 172 has improperly disabled the STP running in network 172 or, the STP has become disabled due to problems just mentioned. As a consequence, even though core network 170 is properly running the STP to avoid loops, since the customer in network 172 is not running the STP, a loop is created in customer network 172 and packets from customer network 172 flood core network 170. As core network 170 and customer network 172 share the same data domain, core network 170 will be flooded with customer packets and will be affected adversely by the customer's action. Yet, it is not possible to ensure that all

network administrators or devices are properly doing their respective jobs and running respective STPs. Provider networks may form the core network for entire countries or even continents. These provider networks should not be affected by fluctuations in customer networks.

Please amend paragraph 0019 at page 7 as follows. (The three changes are in the first and third lines of the paragraph below.)

[0019] ~~In, now pending,~~ In the application NETWORK CONFIGURATION PROTOCOL AND METHOD FOR RAPID TRAFFIC RECOVERY AND LOOP AVOIDANCE IN RING TOPOLOGIES~~,~~ (referenced above), a network configuration protocol allows for de-coupling of customer networks and provider networks running distinct instances of a STP. In brief, in a large ring network comprising first and second rings connected through the shared use of a bridge, the first and second rings are assigned a lower relative priority, e.g. a customer, and a higher relative priority, e.g. a provider. Control packets for the lower priority ring are sent through the entire large ring. Control packets for the higher priority ring are sent only through the higher priority ring. In the event that the shared bridge fails, the lower priority ring maintains its status as its control packets continue to circulate the large ring. The higher priority ring detects the failure and adjusts ports accordingly.

Please amend paragraph 0021 at page 8 as follows. (The changes are in the second line of the paragraph below.)

[0021] A method for resolving this issue is shown in US Patent ~~application~~ Application Serial Number ~~XX/XXX,XXX~~ 10,456,756, entitled "System and Method for Multiple Spanning Tree Protocol Domains in a Virtual Local Area Network" by Rajiv Ramanathan and Jordi MonCada-Elias filed June 9, 2003 with attorney docket number 1988.0140000, the entirety of which is hereby incorporated by reference. In that application, multiple loop detection protocols are provided for each VLAN. This prevents "layer 2" loops by running a customer side spanning tree protocol from a provider network.

Please amend paragraph 0026 at page 9 as follows. (The changes are in the first and second lines of the paragraph below.)

[0026] In accordance with yet another aspect of the invention, ~~is~~ a first network ~~running~~ runs a loop avoidance protocol wherein the root bridge for the first network is disposed in a second network running a distinct loop avoidance protocol instance.

Please amend paragraph 0027 at pages 9-10 as follows. (The changes are in the second and third lines of the paragraph below.)

[0027] In accordance with still yet another aspect of the invention, ~~is~~ a system ~~comprising~~ comprises a first network including a plurality of switches. A second network also includes a plurality of switches. The first and second network are connected by at least a shared switch, the shared switch including a plurality of ports including a second network port connected to the second network. The first network runs a first

loop avoidance protocol instance. The second network does not run the first loop avoidance protocol instance. One of the bridges in the second network controls the state of the second network port.

Please amend paragraph 0032 at page 11 as follows. (The changes are in the second and third lines of the paragraph below.)

[0032] Fig. 8 is a diagram showing the contents of a standard IEEE BPDU, and a T-BPDU in accordance with the invention and an A-BPDU in accordance with one embodiment of the invention.

Please amend paragraph 0038 at page 11 as follows. (The changes are in the first and next to last lines of the paragraph below.)

[0038] Referring now to Fig. 6, there is shown a network 50 operating in accordance with embodiments of the invention. Network 50 is comprised of a core or provider network 52 communicably coupled to a customer network 54 and a customer network 55. Although provider network 52 is shown directly coupled to customer network ~~50~~ 54, clearly networks 52, 54 may be indirectly coupled through other intervening networks.

Please amend paragraph 0046 at page 14 as follows. (The changes are in the first and last lines of the paragraph below.)

[0046] Referring now also to Fig. 8, there ~~is show~~ are shown the different formats for a standard IEEE BPDU 80, a T-BPDU 82 , and an A-BPDU 84. Standard BPDU 80 follows the IEEE 802.1D standard and is used between customer switches in customer

network 54 and provider switches in provider network 52. BPDU 80 is also used between provider switches in provider network 52 ~~and other provider switches in provider network 52~~.

Please amend paragraph 0051 at page 15 as follows. (The change is in the fourth line of the paragraph below.)

[0051] The following explains the operation of the respective switches in provider network 52 when each type of switch receives a BPDU. Switch 56 is the DCB and switches 58 and 60 are non-DCBs. Customer ports are the ports in bridges of provider network 52 that receive information from customer network 54 (e.g. ports 58c and 60c).

Please amend paragraph 0064 at page 17 as follows.

[0064]The actions of each provider switch 56, 58, 60 which receive any BPDU throughout all of network 50 is summarized in Figs. 9-12. Referring to Fig. 9, at step S100, a BDPU is received. At step S102, a query is made as to whether the received BPDU is a standard IEEE BPDU or standard protocol packet. If the answer is yes, control branches to step S2 (Fig. 10). If the answer is no, the software branches to step S104 and queries whether the received BPDU is a T-BPDU. If the answer is yes, control branches to step S20 (Fig. 11). If the answer is no, the software branches to step S108 and queries whether the received BPDU is an A-BPDU. If the answer is yes, control branches to step S40 (Fig. 12). If the answer is no, the packet is dropped at step S110 (Fig. 9).